En busca del perímetro perdido

El cloud, la movilidad y, en los últimos años, el Internet de las cosas, han cambiado los negocios de manera dramática. Han potenciado la conectividad, mejorado la productividad, generado nuevas oportunidades de negocio… y también han incrementado los riesgos. El perímetro, que tan cuidadosamente establecieron los firewalls hace años, ha desaparecido; ya no se trata de proteger una frontera, sino de proteger el dato allá donde vaya o lo utilice quien lo utilice.

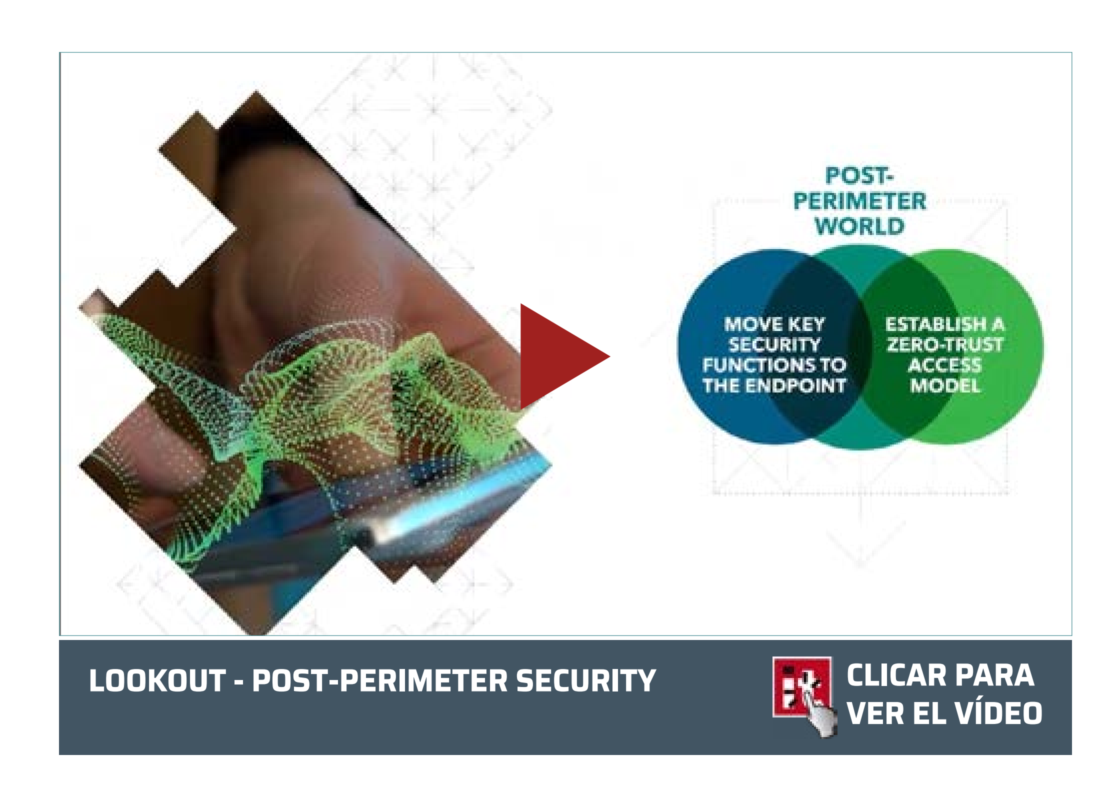
El cambio no es tarea fácil ni se consigue de la noche a la mañana. Los métodos y técnicas de seguridad que eran útiles hace unos años, ya no son de mucha ayuda y eso supone que no hay una consistencia en la seguridad. Entre los cambios no sólo que la superficie de ataque ha crecido, sino que la cantidad y sofisticación de los ataques se ha multiplicado.

En los tiempos del perímetro podría decirse que la vida, el negocio, sólo existía dentro de las paredes físicas de la organización. Se pensaba que si estabas conectado a la red es que eres de confianza, algo echarían por tierra los modelos Zero Trust años después. La seguridad perimetral impedía cosas como la intrusión de redes, el malware, el phishing, las denegaciones de servicio o los ataques de Día Cero; el foco se ponía en la amenaza externa, y se ignoraba por completo el interior.

Pero llegó el momento de salir de esas fronteras. Cargados con sus portátiles, los empleados se convirtieron en nómadas que entraban y salían de las empresas, en ocasiones polinizando malware en sus idas y venidas. Como empleados de pleno derecho quisieron acceder a los recursos empresariales, a las aplicaciones, y la demanda de VPN (redes privadas virtuales) creció. En la época de la confianza, estas conexiones VPN confiaban intrínsecamente en los dispositivos de los usuarios.

El mercado fue evolucionando hasta llegar a la adopción de las aplicaciones SaaS, lo que conllevó que los datos y cargas de trabajo salieran de las empresas. El muro, el perímetro, estaba superado, y la situación no ha hecho sino avanzar. Hoy nuestros archivos, documentos y correos electrónicos están en Office 365 y las arquitecturas son híbridas, lo que significa que parte de nuestros negocios están en Amazon Web Services, en Microsoft Azure, en Google Cloud, o incluso en Alibaba Cloud.

Hacer frente a esta nueva situación en la que el perímetro ha desaparecido supone cambiar la



LOOKOUT - POST-PERIMETER SECURITY

CLICAR PARA VER EL VÍDEO

"No existe el perímetro como tal. Se trata de securizar nuestra forma de trabajar, para que los datos sean consultados y usados por las personas correctas"

Sergio Martínez, Director General, SonicWall Iberia

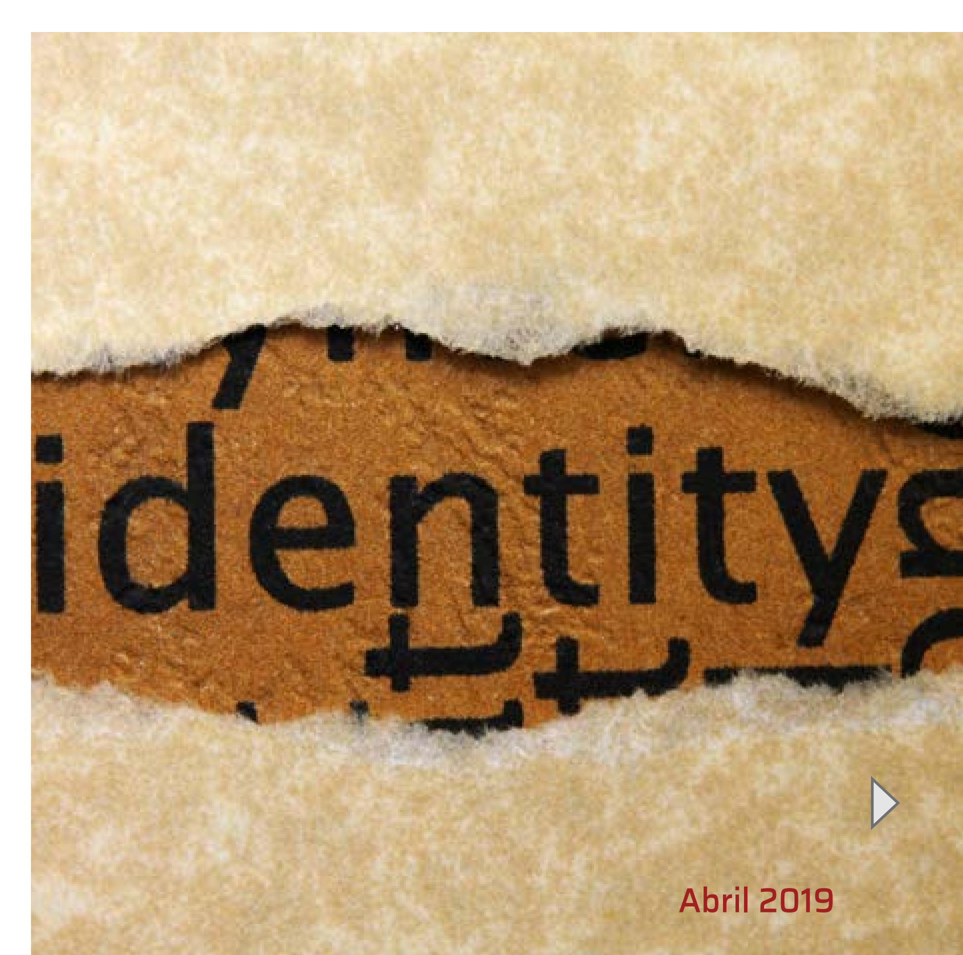
manera en que se protege el dato y se hace frente al riesgo de seguridad. Los firewalls, sistemas de prevención de intrusiones, protección contra el malware funcionan cuando el número de endpoints a proteger es limitado. Ahora no sólo se ha multiplicado el número de puntos finales a administrar, junto con el número de plataformas, sino que es más fácil que nunca compartir datos entre los socios o la propia cadena de suministro. En cuanto al riesgo, los ataques proceden de todas partes: de hacktivistas que buscan notoriedad, de ciberdelincuentes que buscan un beneficio económico, naciones estado en busca de secretos o incluso desde dentro, de empleados descontentos o poco cuidadosos. No es raro que una vez que se adentran en un sistema los ciberdelincuentes estén semanas, meses e incluso años antes de ser detectados copiando datos, robando dinero, trasteando en los sistemas.

El perímetro de la empresa española

"Las empresas siguen invirtiendo en modelos bastión", dice Sergio García, director general de SonicWall para el mercado de Iberia. Dice el directivo que las empresas españolas, especialmente las pequeñas y medianas, son reticentes a ubicar recursos en el cloud a pesar de que los empleados "van por otro lado, y usan Dropbox, Onedrive, Google Drive, G-Suite, etc. Además, el uso de laptops y Smartphones es universal, con conectividad en cualquier lugar, demandando servicios a IT que ahora no tienen…".

Raúl Benito, director general de Qualys, afirma que hace mucho tiempo que la empresa española se ha dado cuenta de que el perímetro ha desaparecido, pero que "se necesitan muchos factores para poder adaptarse a este nuevo ecosistema tecnológico". No sólo menciona el directivo el entender las nuevas tendencias y tecnologías basadas en servicios, flexibilidad, movilidad, etc sino invertir en esta transformación, aquí es donde más nos cuesta con respecto a otras regiones.

Para Juan Rodríguez, director general de F5 Networks en España y Portugal, resulta "curio-



so" que llevando años hablando de la desaparición del perímetro, cuando todas las empresas "deberían haber asimilado ya ese mensaje", sin embargo, una parte importante de las inversiones en seguridad de las organizaciones sigue respondiendo a un modelo tradicional que dejó de tener sentido hace tiempo. "Quizá los proveedores no hemos hecho el esfuerzo suficiente en nuestra comunicación, quizá la resistencia al cambio en las organizaciones es demasiado fuerte", reflexiona el directivo, y añade que a pesar de que la seguridad relacionada con la nube está experimentando incrementos anuales superiores al 50%, todavía vemos que las soluciones de seguridad relacionadas con la infraestructura de TI o con el equipamiento de red siguen representando la mayor parte de la inversión, dejando de lado aspectos clave en el nuevo entorno, como la protección de identidades y la de las aplicaciones.

Sobre el momento en que la empresa española se ha dado cuenta de que no existe el perímetro, dice Juanjo Martínez, Director and GM Southern Europe, Infoblox, que "en muchos casos casi no nos hemos dado cuenta. A medida que se acometen más y más iniciativas de cloud, movilidad, IoT y, en general todas las de transformación digital, esta realidad se revela como mucho más evidente".

Con los procesos de digitalización y la adopción del cloud todo el mundo se pregunta dónde están mis datos, cómo los tengo que proteger; y después llega el cómo y quién. Dice Igor Unanue, director técnico de S21sec, que sí, que las empresas españolas saben que el perímetro es una red cerrada y que tienen que poner el foco más allá de la entrada o salida a Internet, que tienen que tener en cuenta que muchos otros puntos donde ellos tienen parte de su negocio, desde las oficinas remotas, a los subcontratos, a los servidores o aplicaciones en la nube.



"Debemos cambiar el prisma y realizar una revolución en la seguridad en vez de transformarla, pero para eso se necesita tiempo, profesionales adaptados a las nuevas tendencias y por supuesto inversión"

Raúl Benito, Director General, Qualys España y Portugal

¿Cómo se hace frente a la falta de perímetro?

La pérdida de perímetro y lo que cuesta adaptarse a los cambios lleva a retos importantes y datos escalofriantes. Según recoge su último informe sobre Ciberamenazas, SonicWall detuvo el año pasado 10.520 millones de ataques de malware; previsiones de Gartner dicen que para 2020 fracasarán a

la hora de proteger el 75% de los datos sensibles; un estudio de Accenture dice que el tiempo medio para resolver un ataque interno es de 50 días, y 23 días un ataque de ransomware. Cada informe publicado por cada empresa de seguridad indica que las cosas van a peor.

La falta de perímetro es un hecho, aunque son muchas las empresas que aún no han dado un paso al frente para hacer frente a la nueva situación. Algunos expertos hablan de una aproximación de seguridad centrada en el dato y no tanto en los sistemas. Reconociendo que no todos los datos son iguales, sí que tenemos claro que los datos se han convertido en los principales activos de las empresas, lo que a su vez nos lleva a dar prioridad a la Gobernanza del dato, a contar con herramientas para abordar tanto el descubrimiento del datos como su clasificación, almacenamiento y, en lo que aquí respecta, protección.

Parte de esa protección de dato debería centrarse en el autenticación, mejor si es multifactor, para evitar que el dato –que debería estar convenientemente cifrado, no caiga en malas manos. La autenticación va de la mano de la analítica de conducta, el famoso UEBA (User and Entity Behavior Analytics), del aprendizaje automático y otras tecnologías capaces de detectar al intruso. No hay que olvidarla concienciación y formación de los empleados, sobre todo cuando sus acciones son fruto del despiste y la falta de conocimiento y ponen en riesgo a las empresas; mensajes de phishing dirigidos, ataques BEC, acceso a servicios cloud no habilitados por los departamentos de IT o violaciones de políticas son algunos de los retos a los que se deben hacer frente.

Y la empresa española, ¿cómo está haciendo frente a esta falta de perímetro? Dice Sergio Martínez que "están invirtiendo en renovar infraestructura y hacerla más inteligente, que aprenda con las amenazas y que sea capaz de detectarlas por su comportamiento, cada vez los ataques utilizan formas más desconocidas y difíciles de detectar". Es fundamental adoptar el proceso de prevenir, detectar y reaccionar en tiempo real y de forma automática porque el "el

THE PERIMETER IS DEAD. LONG LIVE THE PERIMETERS

CLICAR PARA VER EL VÍDEO

"Una parte importante de las inversiones en seguridad de las organizaciones sigue respondiendo a un modelo tradicional que dejó de tener sentido hace tiempo"

Juan Rodríguez, Director General, F5 Networks España y Portugal

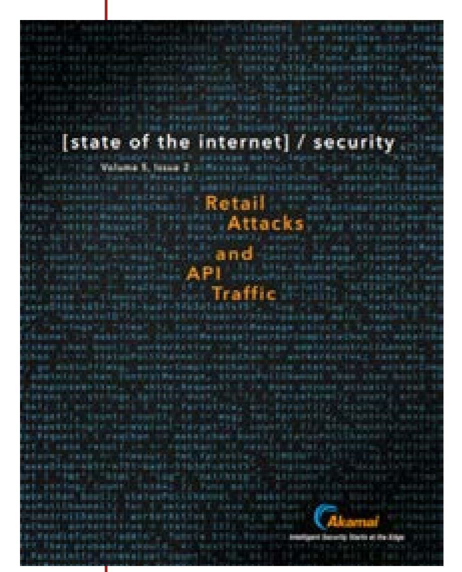
campo de batalla cada vez es más hostil y complejo" y necesitamos de herramientas más sofisticadas para garantizar la supervivencia de las empresas. Continúa el directivo señalando que "el perímetro ha desaparecido, y por ello, hay que construir una defensa en profundidad inteligente".

Dice Raúl Benito que las estrategias que se están adoptando son muy diversas y con foco en distintos ámbitos: gestión del ciclo de vida de las vulnerabilidades, mejora en la detección y prevención de amenazas, protección del dato o gestión de la identidad… depende del nivel de madurez y del presupuesto disponible. "El problema sigue residiendo en que partimos de unas bases que han sido totalmente suplantadas, y por tanto intentamos adaptar nuestros sistemas y nuestras defensas basándonos en conceptos de tiempos pasados. Debemos cambiar el prisma y realizar una revolución en la seguridad en vez de transformarla, pero para eso se necesita tiempo, profesionales adaptados a las nuevas tendencias y por supuesto inversión".

Incrementar la capacidad de vigilancia, implementar las soluciones de seguridad adecuadas y añadir inteligencia a sus sistemas, son los tres frentes en los que las empresas deberían actuar, según Juan Rodríguez, para que "puedan gestionar riesgos y amenazas que tienen que ver con vulnerabilidades, disponibilidad, o integridad de la información".



INFORME SOBRE EL ESTADO DE INTERNET - AKAMAI



Akamai detectó casi 28 mil millones de intentos de relleno de credenciales entre mayo y diciembre de 2018. Los informes sobre el uso de IPv6 pueden no ser correctos, según el análisis de Akamai. Estos son algunos de los aspectos que centran este estudio.

Añade el directivo de F5 Networks que la inversión tecnológica debería orientarse hacia los factores clave que es necesario tener en cuenta para tener éxito en un entorno multicloud: por un lado, reforzar la seguridad de las aplicaciones, incluso de aquellas que no se consideran críticas para el negocio y a las que por ello no se está prestando mucha atención." Garantizar la seguridad de todas las aplicaciones en general y de las aplicaciones nativas Cloud, en particular, es un elemento básico a la hora de orientarse hacia la nube", asegura, explicando que es de vital importancia conocer a fondo la seguridad que ofrece el proveedor cloud y utilizar soluciones que permitan la implantación de políticas de seguridad personalizables. No se olvida de mencionar que otro elemento a tener en cuenta es la autenticación de los usuarios con independencia de su ubicación o del dispositivo que utilicen y la protección de los datos frente a ataques dirigidos.

La primera tendencia que ha tenido la empresa española al hacer frente a la fala de perímetro "ha sido aumentar el número de soluciones de ciberseguridad, cada una especializada en un aspecto concreto: Firewalls, servidores de correo seguro, endpoints, vulnerability assessments, DLPs, NAC, etc.", explica Juanjo Martínez, para después añadir que la tendencia más reciente es apoyarse en un vector que sea transversal a todo, como lo es el DNS. "Seguridad mediante el DNS se está revelando como el medio más efectivo para afrontar esa pérdida de perímetro", dice el directivo de Infoblox.

Dice Igor Unanue que las tecnologías vas más rápido que lo que pensamos, "y cuando hablamos de seguridad más todavía". Dice que hay muchas tecnologías en el mercado, demasiadas, y que la capacidad de asimilación que tienen las empresas de estas tecnologías, es lenta. Dice también el CTO de S21Sec que la tecnología no se está consolidando, que la dispersión, la falta de perímetro "también hace que las tecnologías tengan que ir por nichos, por partes" y que en el futuro contaremos con más modelos de software que con tecnologías de hardware; "hoy tenemos aún mucho hardware conectado que tiene funciones muy activas y responsabilidades importante y en el futuro esto va a ir relegándose al software. Será el software el que tenga la responsabilidad de la seguridad de la base de datos, del tráfico, de todo. Y en ese mo-

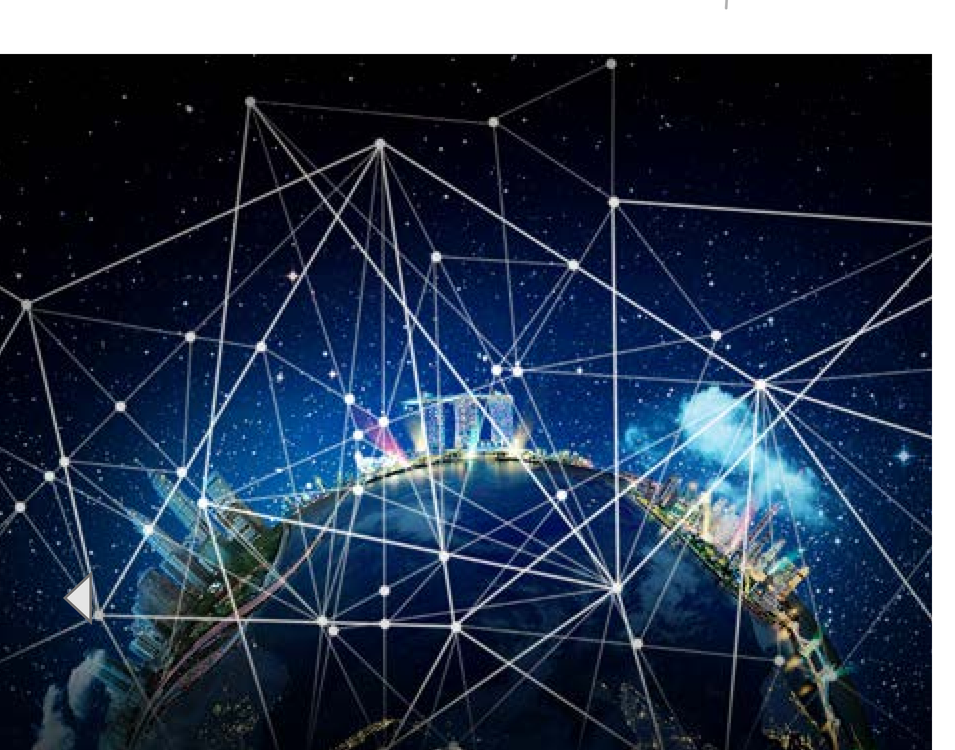
mento será más fácil unificar tecnologías. Ahora mismo necesitamos tecnologías para cada aparato, para cada sistema tecnológico y para cada tipo de aplicación".

El nuevo perímetro

Convencidos de que el dato es el activo más importante, hay quien opina que la mejor manera de protegerlo es crear un perímetro alrededor del

"En muchos casos las empresas aún no se han dado cuenta de que el perímetro no existe"

Juanjo Martínez, Director and GM Southern Europe, Infoblox



¿Dónde está el perímetro?

Ya hemos comentado que hay quien opina que nuevo perímetro está en el dato, mientras que otros apuntan a la identidad. ¿Qué piensan nuestros expertos?

Para **Sergio García, de Sonicwall,** ni lo uno ni lo otro. No existe el perímetro como tal. "Se trata de securizar nuestra forma de trabajar, para que los datos sean consultados y usados por las personas correctas. Pero la seguridad va más allá de esto. Hablamos de la propia supervivencia de la empresa en muchos casos, un incidente mal gestionado, sin acceso a datos críticos, puede acabar con la reputación de la compañía y llevarla al abismo".

Raúl Benito, de Qualys, se refiere al perímetro como "un concepto desfasado y cada vez más intangible" y asegura que "el foco y los esfuerzos de la seguridad deben estar en el verdadero valor de las empresas, sus activos, los datos que contienen y la gestión de quién, cuándo y cómo acceden a ellos". Dice también que no debemos perder el tiempo en definir el perímetro sino en definir lo que son nuestros activos y establecer las políticas de seguridad para poder protegerlos. En función de la definición de estos activos, la seguridad residirá en el dato, en la identidad del acceso o en otras variables que sean las más relevantes para proteger el activo definido.

Para **Juan Rodríguez,** "el perímetro es Internet, por lo que la inversión tiene que orientarse a lograr que las aplicaciones permanezcan siempre seguras con independencia de si se ejecutan en la nube o en el centro de datos corporativo". El directivo de F5 Networks rompe una lanza a favor de la nube asegurando que en estos momentos todos los proveedores cloud aportan unas medidas de monitorización y analítica muy potentes que, al final, contribuyen a reforzar la seguridad; "de esta forma, hoy por hoy, puede ser más seguro estar en la nube que fuera de ella. Migrar a la nube permite acceder a un nivel de seguridad mayor y de forma más económica".

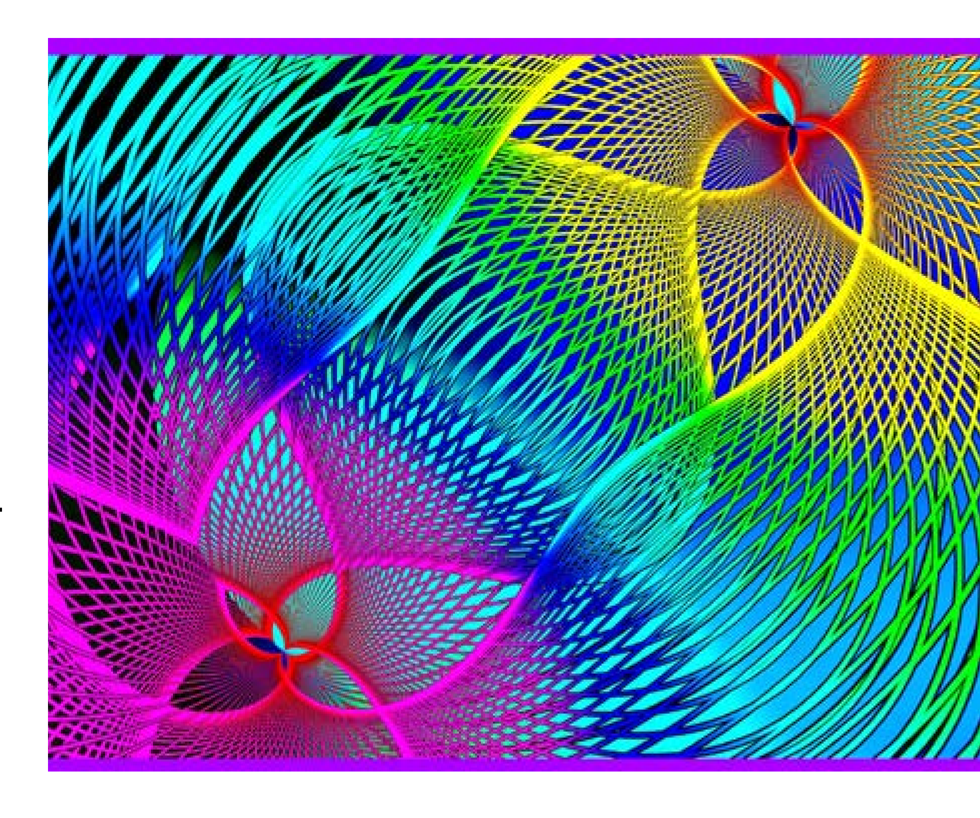
Juanjo Martínez, de Infoblox, también dice que no hay perímetro, ni en el dato ni en la identidad. "Por eso en la medida de lo posible cada elemento de la arquitectura TI y cada desarrollo tiene que llevar la seguridad embebida. No se trata de construir aplicaciones y arquitecturas inseguras, para luego añadirles seguridad perimetral; sino construirlas seguras por diseño en la medida de lo posible. Para los caso en que eso no sea posible o económicamente viable, tenemos las soluciones de seguridad transversales y ubicuas como es la seguridad basada en el DNS".

Sin hablar de perímetros, **Igor Unanue** asegura que no se debe separar la identidad del dato; "van a estar siempre relacionados para poder decidir si te dejo pasar o no. Ahora todos los datos están ahí y lo que hago es dejarte ver unos y otros no".

dato, y no tanto en las localización que lo contienen. El hecho de que prácticamente cada semana se tenga noticia de una brecha de seguridad parece poner de manifiesto que las empresas no cuentan con una política de gestión de datos, de gobernanza, que les permita saber en todo momento qué activos existen y dónde, la relación entre ellos y los sistemas y procesos empresariales, y cómo y de qué manera los datos de las partes autorizadas son usado. Un conocimiento es fundamental para respaldar los esfuerzos para mantener los datos relevantes seguros y privados.

Además, perdido el perímetro se adopta la política del Zero Trust, o Confianza Cero, aplicada no sólo a los usuarios sino a elementos no humanos, como es una aplicación interactuando como sistemas operativos o un proceso de negocio en el que bots estén almacenando y accediendo a datos sensibles.

Para otros, en lugar de intentar construir un muro alrededores de un sistema, lo que hacen en centrarse en los dispositivos, en los endpoints. El famoso BYOD (Bring Your Own Device) y el Internet de las cosas han puesto de manifiesto que el dispositivo en sí mismo es el elemento más vulnerable. De forma que se busca crear una barricada en torno al endpoint, dotarle de más funciones de seguridad que al final aseguren que los usuarios acceden a las aplicaciones cloud sólo desde dispositivos permitidos y desde apps seguras. Este planteamiento también permite que las empresas sean capaces de restringir la capacidad de los usuarios para conectar su dispositivo a un servicio en la nube o software sin soporte o de riesgo.



"La falta de perímetro también hace que las tecnología tengan que ir por nichos, por partes.
No es una tarea fácil"

Igor Unanue, Director Técnico, S21sec

El perímetro no desaparece, sino que se expande. Esta es otras de las opiniones del sector recogidas a través de internet. La explicación es que, habida cuenta del crecimiento de las amenazas internas y de los ataques laterales, quizá tenga más sentido colocar el muro, la defensa, dentro de la propia empresa y no en el exterior o el borde de la misma. De forma que en lugar de un gran muro exterior, debería contemplarse la existencia barreras internas más pequeñas, pero numerosas.

Pero aún hay más, porque para otros el nuevo perímetro está en la identidad. Es decir, hay



Enlaces de interés…

- Zero Trust Networks
- El 58% de los profesionales de TI creen que el perímetro de la red es indefendible
- Las iniciativas de IoT, movilidad y cloud dificultan la protección del perímetro de las TI
- Black Cloud viene al rescate del perímetro perdido

que crear un muro en torno a la identidad de los usuarios. La opinión llega respaldada por el gran negocio que hay en torno a la compra venta de credenciales con privilegios. Según datos de McAfee estas credenciales se venden por 10 dólares en la Dark Web, mientras que un estudio de Accenture recoge que el 18% de los empleados en entornos sanitarios están dispuestos a vender datos confidenciales a partes no autorizadas por entre 500 y 1.000 dólares, y que un 24% de empleados conocen a alguien que lo ha hecho.

Las cuentas privilegiadas permiten a los ciberdelincuentes acceder sin ser detectados. Evitarlo es tan fácil como establecer varios factores de autenticación o soluciones que analicen comportamientos y sean capaces de detectar que aunque se estén utilizando las claves correctas, el usuario no es quien dice ser.

Los que respaldan la opinión de que la identidad es el nuevo perímetro dicen que sólo la identidad puede permitir que las empresas aseguren los recursos al tiempo que ofrecen a los usuarios y empleados la comodidad y facilidad que buscan. Argumentan que la identidad extiende la seguridad más allá de los muros tradicionales de las empresas, hacia los smartphones, las tabletas, los servicios o las aplicaciones, incluidas las redes sociales.

En todo caso lo que parece claro es que el perímetro, como era conocido, ha dejado de existir. Y que esta nueva etapa post-perímetro ofrece la flexibilidad de cambiar las técnicas de autenticación, los privilegios de acceso y otros controles en tiempo real en todos los dispositivos administrados, sin importar dónde se encuentren. Y en todo caso siempre nos quedará la inteligencia artificial y el aprendizaje automático, capaces de distinguir entre la actividad rutinaria legítima de la red que ocurre todos los días y algún evento que representa una amenaza de seguridad. ¿Qué nos importa el perímetro?

Compartir en RRSS